



JOHN NAIMO
AUDITOR-CONTROLLER

**COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER**

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

January 19, 2016

TO: Supervisor Hilda L. Solis, Chair
Supervisor Mark Ridley-Thomas
Supervisor Sheila Kuehl
Supervisor Don Knabe
Supervisor Michael D. Antonovich

FROM: John Naimo 
Auditor-Controller

SUBJECT: **U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES OFFICE FOR
CIVIL RIGHTS' INVESTIGATION OF THE SUTHERLAND BREACH**

This is to inform you that on December 28, 2015, the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) closed their investigation of the County with respect to the Sutherland Healthcare Solutions, Inc.'s (SHS) breach. OCR did not issue any sanctions or penalties against the County, and did not require the County to enter into a resolution agreement. No further action is required by the County on this investigation.

This positive outcome could not have been achieved without the collaborative efforts of the HIPAA Compliance Unit, County Counsel, DHS' and DPH's Privacy and Security Officers, the Chief Information Office, and other staff who assisted this Office with the response.

Please call me if you have any questions, or your staff may contact Linda McBride, Chief HIPAA Privacy Officer, at (213) 974-2166.

JN:PH:RGC:LTM

Attachment

c: Sachi A. Hamai, Chief Executive Officer
Mary C. Wickham, County Counsel
Mitchell H. Katz, M.D., Director, Department of Health Services
Cynthia A. Harding, M.P.H., Interim Director, Department of Public Health
Richard Sanchez, Chief Information Officer



DEPARTMENT OF HEALTH & HUMAN SERVICES

Main - (415) 437-8310, (800) 368-1019

TDD - (415) 437-8311, (800) 537-7697

FAX - (415) 437-8329

www.hhs.gov/ocr

OFFICE OF THE SECRETARY

Office for Civil Rights, Pacific Region

90 7th Street, Suite 4-100

San Francisco, California 94103

December 28, 2015

Linda McBride, Privacy Officer
County of Los Angeles
500 West Temple Street, Room 515
Los Angeles, CA 90012

Our Reference Number: 14-177655

Dear Ms. McBride:

On March 6, 2014, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) received a breach notification report from the County of Los Angeles (the covered entity), pursuant to the HITECH Breach Notification Rule, 45 C.F.R. § 164.408 and § 164.414. Specifically, the covered entity reported that on February 5, 2014, Southerland Healthcare Solutions, Inc. (SHS), a business associate, was burglarized and eight desktop computers were stolen from its office located in Torrance, California. The covered entity explained that it was advised by SHS that the files containing electronic protected health information (ePHI) on stolen computers were unencrypted. The total number of covered entity patients impacted by the breach was approximately 338,700. SHS notified the covered entity of the breach on February 6, 2014, and reported it to the Torrance Police department. The covered entity reported that the protected health information (PHI) included: patients' first and last names, address, birth dates, social security numbers, certain medical information, diagnoses for some patients, and billing information. The information reported by the covered entity could reflect violations of 45 C.F.R. §§ 164.502(a) Uses and Disclosures; 164.530(c) Safeguards; 164.308(a)(6)(ii) Security Incident Procedures: Response and Reporting; 164.314(a)(1) Organizational Requirements: Business Associate Contracts; 164.404(a) and (b) Notification to Individuals; 164.406(a) and (b) Notification to Media; and 164.410(a) Notification by the Business Associate.

OCR enforces the Privacy and Security Rules, and also enforces Federal civil rights laws which prohibit discrimination in the delivery of health and human services because of race, color, national origin, disability, age, and under certain circumstances, sex and religion.

OCR requested information from the covered entity regarding the breach incident, its HIPAA policies and procedures and other supporting documentation. In its response, the covered entity explained that SHS provides billing and collection services service for the Los Angeles County Department of Health Services and Department of Public Health. SHS initially identified approximately 168,500 individuals impacted by the breach. On March 27, 2014, SHS confirmed that approximately 170,000 newly identified individuals were impacted by the breach. The covered entity informed OCR that in response to the incident, SHS implemented additional safeguards, both physical and electronic. The covered entity added additional requirements for all business associates that work with PHI to encrypt the information on their portable and workstation devices. The covered entity also added information security requirements to all

business associate agreements including the agreement with SHS. Specifically, the covered entity requires that the business associate implement appropriate measures to secure its systems and data, including PHI, against internal and external threats risks. The covered entity also requires that the business associate continuously reviews and revises measures to address ongoing threats and risks.

Additionally, in response to the incident and corresponding investigation, the covered entity has taken the following corrective action steps toward coming into compliance with HIPAA:

1. Sent written notices to the individuals affected by the breach, pursuant to 45 C.F.R. § 164.404(a);
2. Notified prominent media outlets of the breach, pursuant to 45 C.F.R. § 164.406(a);
3. Notified OCR of the breach, pursuant to 45 C.F.R. § 164.408(b);
4. Offered identity theft protection monitoring, identity theft insurance and fraud restoration services to affected patients;
5. Implemented an encryption requirement for all its computer workstation hard drives containing PHI; and
6. Retrained staff on its HIPAA policies that included response and reporting security incidents.

The Privacy Rule requires covered entities to enter into written contracts or other arrangements with business associates which protect the privacy of PHI; but covered entities are not required to monitor or oversee the means by which their business associates carry out privacy safeguards or the extent to which the business associate abides by the privacy requirements of the contract. The covered entity is not responsible or liable for the actions of its business associates. However, if a covered entity learns about a material breach or violation of the contract by the business associate, it must take reasonable steps to cure the breach or end the violation, and, if unsuccessful, terminate the contract with the business associate. If termination is not feasible (e.g., where there are no other viable business alternatives for the covered entity), the covered entity must report the problem to the Department of Health and Human Services, Office for Civil Rights. See 45 CFR 164.504(e)(1).

With respect to business associates, a covered entity is considered to be out of compliance with the Privacy Rule if it fails to take the steps described above. If a covered entity is out of compliance with the Privacy Rule because of its failure to take these steps, further disclosures of PHI to the business associate are not permitted. In cases where a covered entity is also a business associate, the covered entity is considered to be out of compliance with the Privacy Rule if it violates the satisfactory assurances it provided as a business associate of another covered entity. http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/236.html

If a covered entity engages a business associate to help it carry out its health care activities and

Page 3 of 4
14-177655

functions, the covered entity must have a written business associate contract or other arrangement with the business associate that establishes specifically what the business associate has been engaged to do and requires the business associate to comply with the Rules' requirements to protect the privacy and security of PHI. In addition to these contractual obligations, business associates are directly liable for compliance with certain provisions of the Privacy Rules. <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html>

You are encouraged to visit OCR's website, where you will find educational materials to help you learn more about the HIPAA Security Rule and other sources of standards for safeguarding electronic protected health information.

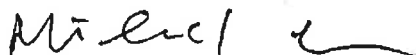
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html>

Based on the foregoing, OCR is closing this case without further action, effective the date of this letter. OCR's determination as stated in this letter applies only to the allegations in this complaint that were reviewed by OCR.

Under the Freedom of Information Act, we may be required to release this letter and other information about this case upon request by the public. In the event OCR receives such a request, we will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

If you have any questions, please do not hesitate to contact Laura Coronado, Investigator, at 415-437-8324 (Voice) or at Laura.Coronado@hhs.gov (Email).

Sincerely,



Michael Leoz
Regional Manager

Additional Resources

Video on conducting a risk analysis:

<http://www.healthit.gov/providers-professionals/video/security-risk-analysis>

OCR guidance on conducting a risk analysis:

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html>

Small provider risk assessment:

<http://www.healthit.gov/providers-professionals/security-risk-assessment>

Instructional video for the small provider risk assessment:

<https://www.youtube.com/watch?v=cZebS00sF00>

The NIST HIPAA Security Rule Toolkit can be helpful for identifying vulnerabilities:

<http://scap.nist.gov/hipaa/>